APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/648,630	08/25/2003	Ernst B. Carter	EXIT-00101	5318

28960   7590   09/26/2008
HAVERSTOCK & OWENS LLP
162 N WOLFE ROAD
SUNNYVALE, CA 94086

EXAMINER
POWERS, WILLIAM S

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
09/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/648,630	CARTER ET AL.
	Examiner	Art Unit	
	WILLIAM S. POWERS	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _03 June 2008_.
2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-45,47-52 and 59-71_ is/are pending in the application.
  4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) _1-45,47-52 and 59-71_ is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on _25 August 2003_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.
  Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
  Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  a)☐ All b)☐ Some * c)☐ None of:
    1.☐ Certified copies of the priority documents have been received.
    2.☐ Certified copies of the priority documents have been received in Application No. _____.
    3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
  * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1.   Applicant's arguments with respect to claims 1-45, 47-52 and 59-71 have been
considered but are moot in view of the new ground(s) of rejection.

Response to Amendment

1.   The Examiner has stated the below column and line numbers as examples. All
columns and line numbers in the reference and the figures are relevant material and
Applicant should be taken the entire reference into consideration upon the reply to this
Office Action.

2.   Claims 1-4, 14-19, 25-27, 30, 36, 37, 40-42, 48, 59, 62 and 64-69 have been
amended.

3.   Claims 46 and 53-58 have been cancelled.

4.   Claims 1-45, 47-52 and 59-71 are pending.

Claim Rejections - 35 USC § 112

5.   The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of
making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the

art to which it pertains, or with which it is most nearly connected, to make and use the same and shall
set forth the best mode contemplated by the inventor of carrying out his invention.

6.   Claims 16, 40, 59 and 60 are rejected under 35 U.S.C. 112, second paragraph,

as being indefinite for failing to particularly point out and distinctly claim the subject

matter which applicant regards as the invention.

        As to claims 16, 40, 70 and 71, it is unclear from the claim language whether an

encryption key or an **encrypted** encryption key is used for the encryption of the file

name and the file contents. According to the claim language, "the key engine further

configured to encrypt the data file contents <u>with</u> the encrypted data file contents key to

generate encrypted data file contents and to encrypt the data file name <u>with</u> the

encrypted data file name key and to encrypt the data file name with the encrypted data

file name key to generate an encrypted data file name" (emphasis added) (claim 16,

lines 5-7). It appears that the data file contents and the data file name are encrypted

with respective **encrypted** data file contents key and **encrypted** data file name key.

The Examiner can find no support for this claim language. In fact, the claim language is

contrary to the specification [0079-0083 and 0107-0108] where the encryption keys are

encrypted after they are used to encrypt the data file contents and the data file name for

security purposes. For purposes of examination, the Examiner assumes that the

respective keys are generated with a pass key or pass phrase supplied by the user,

and are used to encrypt their respective data and are then themselves (the encryption

keys) encrypted before being stored to further secure the keys and the data encrypted

by them. The Examiner finds further support for this assumption at paragraph [0108].

As to claim 59, it appears that limitations of the claim are method steps and not

part of the system of base claim 1. The Examiner will interpret the limitations as the

system configured to.

As to claim 60, the limitations refer to a plurality of file encryption keys, but there

only one file encryption key in the parent claims and is therefore, unclear.

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

8.   The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148

USPQ 459 (1966), that are applied for establishing a background for determining

obviousness under 35 U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.
2.   Ascertaining the differences between the prior art and the claims at issue.
3.   Resolving the level of ordinary skill in the pertinent art.
4.   Considering objective evidence present in the application indicating
      obviousness or nonobviousness.

9.   This application currently names joint inventors. In considering patentability of
the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of
the various claims was commonly owned at the time any inventions covered therein
were made absent any evidence to the contrary. Applicant is advised of the obligation
under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was
not commonly owned at the time a later invention was made in order for the examiner to
consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g)
prior art under 35 U.S.C. 103(a).

10.   Claims 1-5, 9, 12, 19, 20, 26-28, 31, 36, 37, 42, 43, 48-50 and 61-69 are rejected
under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,313,694 to Riedel
et al. (hereinafter Riedel) in view of "Cryptfs: A Stackable Vnode Level Encryption File
System" by Zadok et al. (hereinafter Zadok).

        As to claim 1, Riedel teaches:

        a.   A computer system comprising a memory portion containing an encrypted

                file data (encrypted files are stored) (Riedel, col. 8, lines 24-27) and an operating

                system (UNIX operating system) (Riedel, col. 4, lines 1-12).

Riedel does not expressly mention the kernel of the operating system, but it is inherent

that the operating system has a kernel. However, to forestall any argument, in an

analogous art, Zadok teaches implementing an encryption file system at the kernel level

(Zadok, pg. 1, col. 2, 1st full paragraph).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the secure file system of Riedel with the kernel implementation of Zadok in order to increase performance and offer better security as suggested by Zadok (Zadok, pg. 1, col. 2, 1st full paragraph).

Riedel as modified further teaches:

b.   Configured to decrypt an encrypted directory entry to determine a location of the encrypted data file (decryption of the filename and the i-node pointer) (Riedel, col. 7, lines 30-49) and to decrypt the encrypted data file to access data contained therein (data files can be encrypted for added security) (Riedel, col. 8, lines 21-27).

As to claim 2, Riedel as modified teaches wherein the kernel comprises an encryption engine configured to encrypt clear data files to generate cipher data files, the encryption engine further configured to decrypt the cipher data files to generate clear data files (as evidenced by the encryption and decryption of data files for additional security) (Riedel, col. 8, lines 21-27).

As to claim 3, Riedel as modified teaches the memory portion is coupled to the encryption engine and configured to store the cipher data files (encrypted data files are stored in the storage system) (Riedel, col. 8, lines 21-27).

As to claims 4, 27, 39 and 49, Riedel as modified teaches an encryption engine

is configured to encrypt the clear data files and decrypt the cipher data file according to

a symmetric key encryption algorithm (DES is used which are symmetric key encryption

algorithms) (Zadok, pg. 3, sec. 2.2).

As to claims 5, 9, 28, 37 and 50, Riedel as modified teaches the symmetric key

encryption algorithm is based on a block cipher (DES cipher block chaining) (Zadok, pg.

3, sec. 2.2).

As to claim 12, Riedel as modified teaches the kernel comprises a UNIX

operating system (UNIX operating system) (Riedel, col. 4, lines 1-12).

As to claim 19, Riedel as modified teaches further comprising a secondary

device coupled to the memory, wherein the secondary device stores the encrypted data

file and is accessed using a file abstraction (The distributed computer system of the

patent can be embodied with multiple storage nodes (secondary stores) (Riedel, fig. 1,

ref. 106). The UNIX operating system treats files as abstractions as mentioned in

Applicant's specification [0084] and UNIX is the operating system used by the Riedel

patent) (Riedel, col. 1, lines 14-22 and col. 4, lines 1-12).

As to claims 20, 31 and 43, Riedel as modified teaches the secondary device is a

backing store (data storage) (Riedel, fig. 1, ref. 106 and associated text).

As to claim 26, claim 26 substantially encompasses the limitations present in claims 1, 2, 3 and 19 above and is similarly rejected.

As to claim 36, claim 36 is a method claim substantially encompassing the system claim limitations of claims 1, 2, 3 and 4 above and is similarly rejected.

As to claim 42, Riedel as modified teaches executing kernel code to encrypt the clear data file is performed when data is transferred between a computer memory and a secondary device (files are encrypted before transferring to maintain security of the files) (Zadok, Abstract).

As to claim 48, claim 48 substantially encompasses the limitations of claims 1-3 and is similarly rejected.

As to claims 61-69, Riedel as modified teaches an encrypted directory with file names and i-nodes (file names and i-nodes are encrypted, the i-nodes include location information) (Riedel, col. 4, lines 1-67).

11.   Claims 6-8, 11, 14, 15, 29, 38, 39, 51 and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,313,694 to Riedel et al. (hereinafter Riedel) in view of "Cryptfs: A Stackable Vnode Level Encryption File System" by Zadok et al.

(hereinafter Zadok) as applied to claim 1 above, and further in view of US Patent

Application Publication No. 2003/0005300 to Noble et al. (hereinafter Noble).

As to claims 6, 29, 38 and 51, Riedel as modified does not expressly mention the

Rijndael algorithm. However, the Rijndael algorithm is old and well known in the art at

the time of Applicant's invention as evidenced by Noble. Noble teaches the symmetric

key encryption algorithm comprises Rijndael algorithm (Noble, [0090]).

Therefore, one of ordinary skill in the art at the time the invention was made

would have been motivated to implement the secure file system of Riedel as modified

with the use of the Rijndael algorithm in order to take advantage of its excellent

performance characteristics as suggested by Noble (Noble, [0090]).

As to claim 7, Riedel as modified teaches the symmetric key encryption algorithm

uses a block size of 128 bits (block size of 16 byte) (Noble, [0091]).

As to claim 8, Riedel as modified teaches the symmetric key encryption algorithm

uses a key length of 128 bits (key size of 16 byte) (Noble, [0091]).

As to claims 11 and 39, Riedel as modified teaches the symmetric key encryption

algorithm comprises Blowfish (Blowfish is used as a symmetric key encryption

algorithm) (Noble, [0119]).

As to claim 14, Riedel as modified teaches wherein the memory portion comprises a first logical protected memory configured to store encrypted data files and a second logical protected memory configured to store encrypted key data (decryption keys are not stored with the encrypted files) (Riedel, col. 5, line 63-col. 6, line 3) (encrypted keys are stored in memory) (Noble, [0047, 0051-0054]).

As to claim 15, Riedel as modified teaches an encryption key management system configured to control access to the encrypted data files and the encrypted key data (use of authentication token to control access to encrypted files and respective encrypted keys) (Noble, Abstract).

As to claim 52, Riedel as modified teaches the kernel comprises a UNIX operating system (UNIX operating system) (Riedel, col. 4, lines 1-12).

12.   Claims 10 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,313,694 to Riedel et al. (hereinafter Riedel) in view of "Cryptfs: A Stackable Vnode Level Encryption File System" by Zadok et al. (hereinafter Zadok), and further in view of US Patent Application Publication No. 2003/0005300 to Noble et al. (hereinafter Noble) as applied to claim 5 above, and further in view of US Patent No. 5,903,881 to Schrader et al. (hereinafter Schrader).

As to claim 10, Riedel as modified does not expressly mention the use of the Triple-DES encryption algorithm. However, in an analogous art, Schrader teaches the symmetric key encryption algorithm comprises a Triple-DES algorithm (Schrader, col. 17, lines 12-21).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the secure file system of Riedel as modified with the use of the Triple-DES algorithm of Schrader in order to provide security for transactions as suggested by Schrader (Schrader, col. 17, lines 12-21).

As to claim 30, Riedel as modified teaches wherein one or more of the encryption keys comprises at least 1,024 bits (Schrader, col. 17, lines 12-21).

13.   Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,313,694 to Riedel et al. (hereinafter Riedel) in view of "Cryptfs: A Stackable Vnode Level Encryption File System" by Zadok et al. (hereinafter Zadok) as applied to claim 12 above, and further in view of US Patent No. 5,727,206 to Fish et al. (hereinafter Fish).

As to claim 13, Riedel as modified does not expressly mention the version of UNIX that is used. However, in an analogous art, Fish teaches wherein the UNIX operating system is a System V-Revision (file system operates in a UNIX SVR4 environment) (Fish, col. 12, lines 22-32).

Therefore, one of ordinary skill in the art at the time the invention was made

would have been motivated to implement the secure file system of Riedel with the

system v-revision UNIX environment of Fish because the use of vnodes makes

integration more seamless as suggested by Fish (Fish, col. 12, lines 22-32).

14.   Claims 16-18, 25, 40, 70 and 71 are rejected under 35 U.S.C. 103(a) as being

unpatentable over US Patent No. 7,313,694 to Riedel et al. (hereinafter Riedel) in view

of "Cryptfs: A Stackable Vnode Level Encryption File System" by Zadok et al.

(hereinafter Zadok) as applied to claim 15 above, and further in view of "A

Cryptographic File System for UNIX" by Blaze.

As to claims 16 and 40 as best understood, Riedel as modified teaches

encrypting the file name and the file contents, but does not provide the details of the

encryption scheme   (Riedel, Abstract and col. 8, lines 21-27). However, in an

analogous art, Blaze teaches:

> a.   Wherein the encryption key management system comprises a key engine
>
> (encryption engine is used to generate keys and encrypt/decrypt data) (Blaze,
>
> pg. 9, sec. 1.1, 2nd paragraph).
>
> Therefore, one of ordinary skill in the art at the time the invention was made

would have been motivated to implement the secure file system of Riedel as modified

with the encryption engine of Blaze in order to achieve a secure, transparent

encryption/decryption file system as suggested by Blaze (Blaze, Abstract).

Riedel as modified further teaches:

b.   The key engine configured to receive a pass key and a data file name to generate an encrypted data file name key (keys are generated by pass phrases (pass key) input by the user which are used to encrypt the file name and the file contents) (Blaze, pg. 11, sec. 2.2, 4th paragraph and pg. 13, sec. 3).

c.   The key engine further configured to use the encrypted data file name key and data file contents to generate an encrypted data file contents key (keys are generated by pass phrases (pass key) input by the user which are used to encrypt the file name and the file contents) (Blaze, pg. 11, sec. 2.2, 4th paragraph and pg. 13, sec. 3).

d.   The key engine further configured to encrypt the data file contents with the encrypted data file contents key to generate encrypted data file contents (file contents encrypted) (Blaze, pg. 13, sec. 3) and to encrypt the data file name with the encrypted data file name key to generate an encrypted data file name (file names are encrypted) (Blaze, pg. 12, col. 1, last paragraph).

As to claim 17, Riedel as modified teaches wherein the encryption key management system is configured to store the encrypted data file name, wherein the data file name is associated with the encrypted file contents (encrypted file names are used to access encrypted file contents) (Riedel, Abstract).

As to claim 18, Riedel as modified teaches wherein the encryption key management system is further configured to grant access to a data file if a corresponding access permission of the data file is a predetermined value (files are accessed through one of two keys or both) (Riedel, col. 5, lines 5-52).

As to claim 25, Riedel as modified teaches wherein the encryption key management system is further configured to encrypt a pathname to the encrypted data file, the encryption key management system further configured to decrypt the pathname to the encrypted data file when retrieving encrypted data file contents (encrypted path names) (Blaze, pg. 11, sec. 2.2, 3rd paragraph).

As to claim 70, claim 70 substantially encompasses the limitations present in claims 1, 2, 3, 16 and 19 and is similarly rejected.

As to claim 71, claim 71 substantially encompasses the limitations present in claims 1, 2, 3, 4 and 16 and is similarly rejected.

15.   Claims 21, 32 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,313,694 to Riedel et al. (hereinafter Riedel) in view of "Cryptfs: A Stackable Vnode Level Encryption File System" by Zadok et al. (hereinafter Zadok) as applied to claim 19 above, and further in view of US Patent No. 6,836,888 to Basu et al. (hereinafter Basu).

As to claims 21, 32 and 44, Riedel as modified does not expressly mention the use of a swap device, but using a swap device is old and well known in the art as evidenced by Basu. Basu teaches wherein the secondary device is a swap device (swap device) (Basu, col. 11, lines 33-55).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the secure file system of Riedel as modified with the swap device of Basu in order to control the flow of information as suggested by Basu (Basu, col. 1, lines 9-14).

16. Claims 22-24, 33-35, 45 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,313,694 to Riedel et al. (hereinafter Riedel) in view of "Cryptfs: A Stackable Vnode Level Encryption File System" by Zadok et al. (hereinafter Zadok) as applied to claim 19 above, and further in view of US Patent No. 6,477,545 to LaRue.

As to claims 22 and 33, Riedel as modified does not expressly mention an interface port comprising a socket connection. However, a socket connection and port are old and well known in the art as evidenced by LaRue. LaRue teaches an interface port comprising a socket connection (sockets are used for communication between nodes of a network) (LaRue, col. 6, line 56-col. 7, line 25).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the secure file system of Riedel as modified with the socket connections of LaRue in order to manage information within a network as suggested by LaRue (LaRue, col. 1, lines 47-52).

As to claims 23, 34 and 45, Riedel as modified teaches the socket connection comprises a computer network (socket connection connects different devices in a computer network) (LaRue, col. 6, line 56-col. 7, line 25).

As to claims 24, 35 and 47, Riedel as modified teaches the computer network comprise the Internet (LaRue, col. 6, line 56-col. 7, line 25).

17.   Claim 41 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,313,694 to Riedel et al. (hereinafter Riedel) in view of "Cryptfs: A Stackable Vnode Level Encryption File System" by Zadok et al. (hereinafter Zadok) as applied to claim 40 above, and further in view of US Patent Application Publication No. 2003/0005300 to Noble et al. (hereinafter Noble).

As to claim 41, Riedel as modified does not expressly mention specific storage areas. However, in an analogous art, Noble teaches storing the encrypted data file name key and the encrypted file contents key in a first protected area of computer storage and storing the encrypted data file name and the encrypted file contents in a

second protected area of the computer storage (decryption keys are not stored with the

encrypted files) (Riedel, col. 5, line 63-col. 6, line 3) (encrypted keys are stored in

memory) (Noble, [0047, 0051-0054]).

Therefore, one of ordinary skill in the art at the time the invention was made

would have been motivated to implement the secure file system of Riedel as modified

with the encrypted key storage of Noble in order to maintain the security of computer

data as suggested by Noble (Noble, [0003]).

18.   Claim 59 and 60 are rejected under 35 U.S.C. 103(a) as being unpatentable over

US Patent No. 7,313,694 to Riedel et al. (hereinafter Riedel) in view of "Cryptfs: A

Stackable Vnode Level Encryption File System" by Zadok et al. (hereinafter Zadok) as

applied to claim 1 above, and further in view of US Patent No. 6,938,166 to Sarfarti et

al. (hereinafter Sarfarti).

As to claim 59, Riedel as modified teaches:

a.   One of encrypting and decrypting a data file in the directory with a

corresponding file encryption key (the encryption and decryption of data files for

additional security) (Zadok, pg. 4, col. 1, 5th paragraph).

Riedel as modified teaches encrypting directory entries, but does not expressly mention

encrypting the directory itself. However, in an analogous art, Sarfarti teaches:

b.   One of encrypting and decrypting the directory with a directory encryption

key (signing and encrypting the directory) (Sarfarti, Abstract and col. 5, line 66-

col. 6, line 28).

Therefore, one of ordinary skill in the art at the time the invention was made

would have been motivated to implement the secure file system of Riedel as modified

with the directory encryption of Sarfarti in order to enable a conditional access of data

as suggested by Sarfarti (Sarfarti, col. 9, lines 45-55).

As to claim 60, Riedel as modified teaches wherein in the corresponding file

encryption keys are different (different files have different keys or combinations of keys)

(Riedel, col. 4, lines 30-55).

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to WILLIAM S. POWERS whose telephone number is

(571)272-8573. The examiner can normally be reached on m-f 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/W. S. P./   William S. Powers
Examiner, Art Unit 2134   Examiner
                                                         Art Unit 2134

9/24/2008

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2134